Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0364-2007

for

Vanguard Enforcer
Version 7 Release 1

from

Vanguard Integrity Professionals, Inc.

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0364-2007

Vanguard Enforcer Version 7 Release 1

from

Vanguard Integrity Professionals, Inc.

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3 augmented by** **ALC_FLR.1 – Basic flaw remediation**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 08 March 2007

The President of the Federal Office
for Information Security

IT Security Certified

Dr. Helmbrecht L.S. SOGIS - MRA

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement has been signed by the national bodies of:

Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Vanguard Enforcer, Version 7 Release 1 has undergone the certification procedure at BSI.

The evaluation of the product Vanguard Enforcer, Version 7 Release 1 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Vanguard Integrity Professionals, Inc.
6625 South Eastern Ave, Suite 100
Las Vegas, NV 89119-3930
USA

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 08 March 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described as specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product Vanguard Enforcer, Version 7 Release 1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Vanguard Integrity Professionals, Inc.
6625 South Eastern Ave, Suite 100
Las Vegas, NV 89119-3930
USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Vanguard Enforcer Version 7 Release 1 (also called Vanguard Enforcer Version 7.1.1 in the following) provides administrative support for the IBM Resource Access Control Facility (RACF) Security Server, running on the IBM z/OS V1R6 operating system executing in an abstract machine on an IBM zSeries processor.

The product is intended to provide automated surveillance and optional control of the z/OS RACF profiles and settings. Enforcer monitors the RACF configuration settings and modifies them (using the RACF SETROPTS command) via the 'Security Server Options Settings’. This includes RACF configuration settings, RACF profile definitions, and select system configurations (APF list, Link List, Program properties table, SVC definitions).

Vanguard Enforcer monitors selected installation defined settings and operating system settings. When discrepancies are found Enforcer will perform one or more of the following operations:

- Log the discrepancy.
- Notify pre-determined administrators of the discrepancy.
- Optionally take automatic corrective action to restore the system to the baseline configuration, where a “baseline” is a set of the values that represent the system settings in the correct configuration.

Vanguard Enforcer is accessed via the following interfaces:

- z/OS Operator Console: The MVS operator command interface is used to start, stop and modify the operating characteristics of Enforcer.
- Interactive System Productivity Facility (ISPF) Interface: The The ISPF interface allows the administrator to perform the operations needed to configure Enforcer.

The IT product Vanguard Enforcer, Version 7 Release 1 was evaluated by atsec information security GmbH. The evaluation was completed on 07 February 2007. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Vanguard Integrity Professionals, Inc.
6625 South Eastern Ave, Suite 100
Las Vegas, NV 89119-3930
USA

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL3 (Evaluation Assurance Level 3 augmented by ALC_FLR.1). The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL3	TOE evaluation: methodically tested and checked
+: ALC_FLR.1	Life cycle support – Basic flaw remediation

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FAU	**Security Audit**
FAU_ARP.1	Security audit automatic response
FMT	**Security Management**
FMT_SMF.1	Specification of Management Functions

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	**Addressed issue**
FAU	**Security Audit**
FAU_SAA.5-RACF	RACF Potential Violation Analysis

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.2.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FDP	**User Data Protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA	**Identification and Authentication**
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT	**Security Management**
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static Attribute Initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT	**Protection of the TSF**
FPT_SEP.1	Domain Seperation
FPT_STM.1	Reliable Time Stamps

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.5.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
F.AU	**Audit**
F.AU.1	Sensor violation analysis and automatic response
F.MGMT	**TOE Management**
F.MGMT.1	Security Administrators may perform Enforcer customization.
F.MGMT.2	Security Administrators define and select RACF profiles monitored.
F.MGMT.3	Security Administrators may select or deselect options for automatic RACF profile correction
F.MGMT.4	Security Administrators may select general security options
F.MGMT.5	Security Administrators may select notification recipients

Table 5: Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

No SOF claims are made for this evaluation.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The following threat must be countered by security functions implemented by the TOE:

T.ADMINISTRATIVE_ERROR: Due to the complexity of and changes to RACF profiles and administrators are asumed to be trustworthy and trained, deviations to a designated system configuration may arise. The purpose of the TOE is to provide a baseline data set of the security settings that can be used to make comparisons to RACF profiles and system configurations on an ongoing basis so changes may be detected.

The ST [6] describes the following organisational security policies the TOE must comply with:

- **P.RACF_MONITOR_ROLLBACK**: The RACF Security Server database profiles and select system configurations shall be monitored for changes from the predefined baseline; the default action for detected changes shall be to roll back changes to a known state as defined in the baseline data set.
- **P.RACF_MONITOR_NOTIFY**: The RACF Security Server database shall be monitored for changes from the predefined baseline; notices of detected changes shall be sent to the designated administrator.

1.5 Special configuration requirements

The Target of Evaluation, Vanguard Enforcer Version 7.1.1, requires the „Vanguard Date Code Software“ element to be installed. For other components that are installed automatically please refer to chapter 5.

Additionally, the TOE is required to run on IBM zSeries hardware equivalent to the Common Criteria evaluated configuration of the zSeries operating system as described in [12], restricted to the Discretionary Access Control mode of operation. All required, optional, and restricted software configurations described in that document must be followed.

Vanguard Enforcer Version 7.1.1 requires the following PTFs (Program Temporary Fixes) to be installed (please refer to [11]): VED6306, VED6301, VED6300, VED6299, VED6298, VED6297, VED6296, VED6294, VED6293, VED6291, VED6290, VED6285, VED6284, VED6283, VED6279, VED6277, VED6272, VED6259.

1.6 Assumptions about the operating environment

The following assumptions about the environment of the TOE are made:

- **A.AUTHORIZE**: Procedures exist for granting only authorized users access to TOE controls.
- **A.TIMESTAMP**: The environment will provide reliable timestamps.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Vanguard Enforcer, Version 7 Release 1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Vanguard Enforcer product	Version 7, Release 1	Tape
2	SW	PTFs: VED6306, VED6301, VED6300, VED6299, VED6298, VED6297, VED6296, VED6294, VED6293, VED6291, VED6290, VED6285, VED6284, VED6283, VED6279, VED6277, VED6272, VED6259		Tape
3	DOC	Vanguard Enforcer™ Administrator Guide	November 2006	PDF (VENF-111606-710U)
4	DOC	Vanguard Security Solutions™ Installation Guide	November 2006	PDF (VSS-111606-710I)
5	DOC	Vanguard Enforcer™ Secure Installation and Operations for Common Criteria	November 2006	PDF (VENF-111606-710I)

No	Type	Identifier	Release	Form of Delivery
6	DOC	Vanguard Enforcer™ Cover Letter for Common Criteria		PDF (VENFC -111606-710C)

Table 6: Deliverables of the TOE

3 Security Policy

The Vanguard Enforcer provides administrative support for the IBM Resource Access Control Facility (RACF) Security Server.

Therefore its main purose is to provide mechanisms for security audit and security management.

The security policy of the TOE is defined by the following TOE security functional requirements:

- SFR components of the class FAU define the mechanisms for security audit and the reaction of the TOE in case of a violation of a predefined system configuration.
- SFR components of the class FMT define the management functions the TOE provides.

4 Assumptions and Clarification of Scope

The security aspects of the environment in which the TOE is expected to be used are described in terms of assumptions. The assumptions for the environment are divided into assumptions about the intended usage of the TOE and assumptions about the environment the TOE is going to be used in.

4.1 Usage assumptions

- **A.ADMINISTRATION**: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains, however, no assumption is made that an administrator cannot make errors.
- **A.NO_EVIL_ADM**: The personnel responsible for the administration of the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- **A.SECURITY_ADMINISTRATOR**: There will be an individual assigned to administer TOE security that is different that the individual assigned to administer IT environment security. The intention is to have the administration of TOE security functions separated from that of the IT environment security administration, thereby preventing one administrator from duplicating errors made in the setup of the IT environment RACF database and the TOE baseline data set.

4.2 Environmental assumptions

- **A.MULTIPLE_SENSOR_SESSION**: The administration of multiple TOE Sensor sessions must ensure each is session monitors different aspects of the system and that overlap between sessions is eliminated.
- **A.UNAUTHORIZED_ACCESS**: The TOE code, configuration, audit files, log files, and baseline data sets are protected from unauthorized access using the access control functions of the underlying operating system.
- **A.CAPP_MODE**: z/OS as part of the IT environment is operated using only Discretionary Access Control (as defined by the z/OS Security Target); the use of Mandatory Access Control is not allowed.
- **A.LOCATE**: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access to the hardware the TOE is running on.
- **A.PROTECT**: The TOE software, which is critical to security policy enforcement, will be protected from unauthorized modification.

4.3 Clarification of scope

The TOE environment must comply with the following OSP:

- **PE.AUTHORIZED_USERS**: The TOE environment must ensure that only those users who have been authorized to access the information within the system may access the system and the TOE code and configuration data sets are protected from unauthorized access.
- **PE.AUTHENTICATE**: The TOE environment must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources. Such limited access to the TOE is configured by the administrator and should be conformant with the security policies of the organization responsible for the operations of the TOE.
- **PE.MANAGE**: Those responsible for the TOE environment must ensure that the underlying operating system and hardware is configured and managed in a secure way.
- **PE.INSTALL**: Those responsible for the TOE environment must ensure that the TOE is installed in a secure manner, as specified in the Installation, Generation, and Secure Installation guidance.

5 Architectural Information

The TOE is comprised of Startup code, Option Interface code, Sensor code, Vanguard Date Code Software, and guidance documentation. The TOE is intended to be used as an audit tool on an IBM zSeries z/OS system.

This means in detail that the TOE software is comprised of the following major components:

1. Startup and Option Interface Components
    a. Enforcer REXX execs (Restructured Extended Executor executable code)
    b. Enforcer ISPF Dialogs
2. Sensor Component
    a. The Sensor Task
3. Vanguard Date Code Software

The Sensor Task is used to monitor the system wide options and the RACF security server database, detect changes to selected profiles, and by default, rollback changes, where possible, to the settings contained in a data set that is generated specifically to establish a “baseline” set of the values that represent the system settings in the correct configuration.

Multiple TOE Sensor Tasks (or sessions) may be run concurrently; however, each must maintain its own required baseline data set.

The TOE requires that Vanguard Date Code Software validate the Enforcer software license prior to and during execution, and although it is part of the TOE, it has no security functionality.

The following figure - TOE and TOE Environment - shows the major components of TOE software within its intended environment, although it is not intended to be a detailed representation of the product, but is intended to show the general structure only. It shows only one Sensor Task, as all TOE Sensor tasks act independently without knowledge of or communication to others. The administration of multiple TOE Sensor tasks must ensure each is monitoring different aspects of the system and overlap is eliminated.

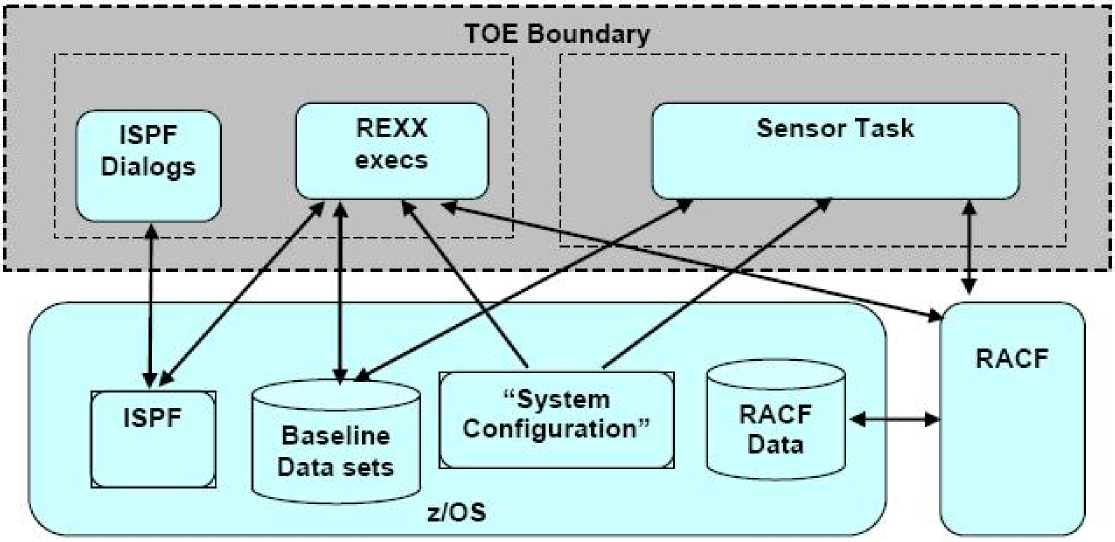

Figure 1: TOE and TOE Environment

6 Documentation

For a listing of the documentation delivered with the TOE please refer to chapter 2 or chapter 14 of this report.

7 IT Product Testing

7.1 Developer testing

TOE test configuration: The TOE was tested on a system equivalent the evaluated configuration described in the Security Target for IBM z/OS Version 1 Release 6 [12] with the following specifications:

xSeries 255 with 3.0 GHz processors (4), and

- RedHat Linux base OS
- FLEX-ES z/Series emulation software[9]
- z/VM 4.4 (64bit)
- z/OS 1.6 EAL3 Certified OS

The evaluated configuration was installed following the guidance in the Secure Installation and Operations for Common Criteria manual, the Installation Guide and Administrators Guide ([8]-[11]).

[9] FLEX-ES is a software-based emulation of a z/Series mainframe. FLEX-ES runs on Intel based architectures and allows to execute z/OS on top of it without any necessary modifications or configuration particularities. It was ensured that the FLEX-ES establishes an equivalent implementation of the z/Architecture to fulfil the requirements of z/OS.

Testing approach: The developer employed the strategy to create specific individual test cases for each TSF aspect modeled in the Security Target. This resulted in every sensor being thoroughly tested: all potential discrepancies that a sensor would be able to identify between system configuration and Enforcer's baselines are covered by the tests. All aspects of the security management functionality defined in the ST are covered as well, including all relevant configuration options for the TOE. Positive verification testing was augmented by negative testing (for example, making sure that the TOE does not accept values out of the specified range).

Test cases in general are executed manually, with JCL scripts supporting the configuration and de-configuration of conditions in the underlying system. The relevant interfaces have been triggered directly and indirectly as appropriate.

Test results: Test results were observed by analysis of the output generated by the TOE in its log file and via emails to administrators, and if necessary by verifying that the TOE had taken the corrective action in the underlying system as expected. All tests have been successfully executed.

7.2 Evaluator testing

TOE test configuration: The TOE was tested on the same system used for developer testing.

Independent testing covered aspects of all TOE SFRs and security functions.

The security functions tested by independent tests include:

- F.AU.1.1 - System APF Sensor
- F.AU.1.2 - System Critical Data Sets Sensor
- F.AU.1.4 - Access List Expiration Processing Sensor
- F.AU.1.8 - System Program Properties (PPT) Sensor
- F.AU.1.11 - System Security Server Options Sensor
- F.AU.1.13 - System SVC Sensor
- F.AU.1.15 - Installation Critical Data Set Profiles Sensor
- F.MGMT.1 - TSF administration
- F.MGMT.3 - Warning/nowarning mode

The evaluator demonstrated that a reasonable sample size of developer tests have been witnessed. Selection criteria included functions that were noticed during the course of the evaluation as being of particular interest to the evaluators, tests covering both typical and untypical sensor architectures, and the coverage of both management and sensor functionality.

Test results: Aspects of all SFRs were represented in the sample. All tests have been successfully executed.

7.3 Penetration testing

While some of the penetration tests devised by the evaluator directly address security functional behavior as specified in the ST, a number of penetration tests were carried out that targeted the TOE architecture as a whole rather than individual security functions. This included aspects like the internal scheduling of sensor execution and suspected concurrency issues. The evaluators devised both automated as well as manual tests, as appropriate, and carried them out in conjunction with the independent test activities.

The security functions tested during penetration testing include:

- F.AU.1.3 - Installation Critical Groups Sensor
- F.AU.1.5 - Installation Critical General Resource Profiles Sensor
- F.AU.1.6 - System Link List Sensor
- F.AU.1.13 - System SVC Sensor
- F.AU.1.14 - Installation Critical DASD Volumes Sensor
- F.MGMT.1 - TSF administration

As a result of the evaluation, no exploitable obvious vulnerabilities and no residual vulnerabilities for the TOE in its intended environment were identified.

8 Evaluated Configuration

The evaluated version of the TOE is Vanguard Enforcer 7.1.1 as described in the ST [6]. The TOE has to be set up in accordance to the guidance documentation as described in chapter 2 of this report and the Security Target. Both the developer and the evaluator have tested the TOE on an underlying system equivalent the evaluated configuration described in the Security Target for IBM z/OS Version 1 Release 6 [12] with the following specifications:

xSeries 255 with 3.0 GHz processors (4), and

- RedHat Linux base OS
- FLEX-ES z/Series emulation software
- z/VM 4.4 (64bit)
- z/OS 1.6 EAL3 Certified OS

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL3.

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ALC_FLR.1 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	CC Class ADO	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS

Assurance classes and components		**Verdict**
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 7: Verdicts for the assurance components

The evaluation has shown that:

- the Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL3 augmented by ALC_FLR.1

The results of the evaluation are only applicable to the Vanguard Enforcer Version 7.1.1 as described in chapter 2 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [8] - [11] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0364-2007, Version 1.39, 01.12.2006, Vanguard Enforcer™ Version 7.1 Common Criteria Security Target

[7] Evaluation Technical Report, Version 3, 07.02.2007, (confidential document)

[8] Vanguard Enforcer Administrator Guide, Document Number VENF-111606-710U, November 2006

[9] Vanguard Enforcer Secure Installation and Operations for Common Criteria, Document Number VENF-111606-710I, November 2006

[10] Vanguard Security Solutions Installation Guide, Document Number VSS-111606-710I

[11] Cover Letter to Customers who have ordered Vanguard Enforcer 7.1 Common Criteria EAL3+ Evaluated Configuration, Document Number VENFC -111606-710C

[12] Security Target for IBM z/OS Version 1 Release 6, V1.15, February 2005, http://www.commoncriteriaportal.org/public/files/epfiles/0247b.pdf

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	**Assurance Family**
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview (chapter 11.1)

"Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”